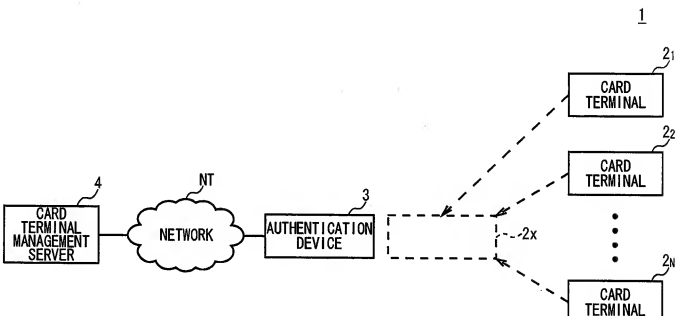

1
2_1
CARD TERMINAL
2_2
CARD TERMINAL
2_N
CARD TERMINAL
2x
4
CARD TERMINAL MANAGEMENT SERVER
NT
NETWORK
3
AUTHENTICATION DEVICE

FIG. 1

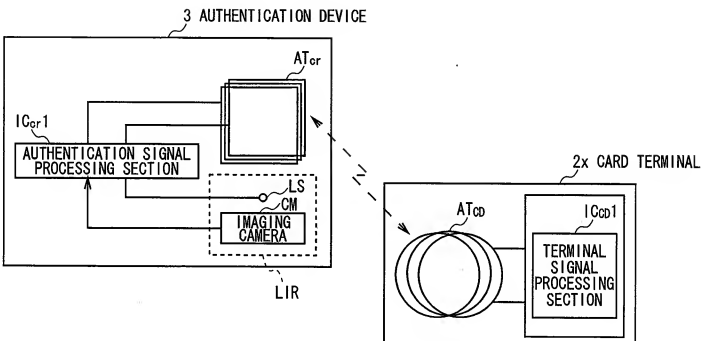

3 AUTHENTICATION DEVICE
ATcr
ICcr1
AUTHENTICATION SIGNAL PROCESSING SECTION
LS
CM
IMAGING CAMERA
LIR
2x CARD TERMINAL
ATCD
ICCD1
TERMINAL SIGNAL PROCESSING SECTION

FIG. 2

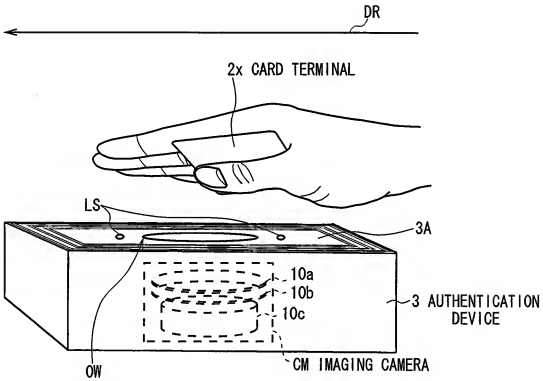

DR
2x CARD TERMINAL
LS
3A
10a
10b
10c
3 AUTHENTICATION DEVICE
OW
CM IMAGING CAMERA

FIG. 3

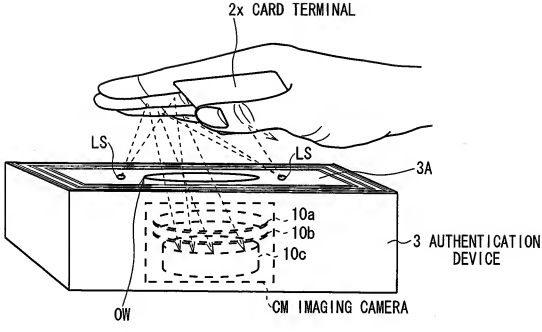

2x CARD TERMINAL
LS
LS
3A
10a
10b
10c
3 AUTHENTICATION DEVICE
OW
CM IMAGING CAMERA

FIG. 4

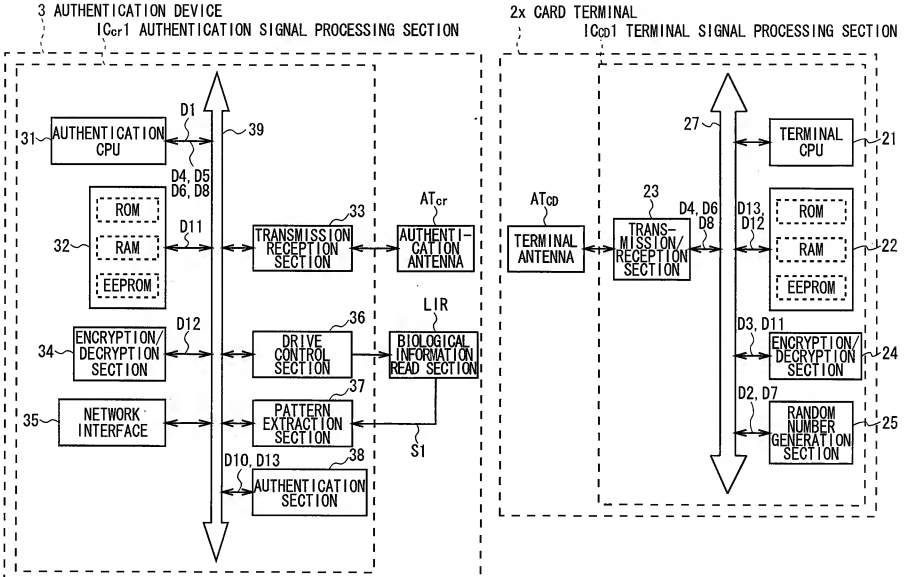

3 AUTHENTICATION DEVICE
ICcr1 AUTHENTICATION SIGNAL PROCESSING SECTION
2x CARD TERMINAL
ICCD1 TERMINAL SIGNAL PROCESSING SECTION
AUTHENTICATION CPU
31
D1
39
D4, D5
D6, D8
ROM
RAM
EEPROM
32
D11
TRANSMISSION RECEPTION SECTION
33
ATcr
AUTHENTI-CATION ANTENNA
ENCRYPTION/ DECRYPTION SECTION
34
D12
DRIVE CONTROL SECTION
36
LIR
BIOLOGICAL INFORMATION READ SECTION
NETWORK INTERFACE
35
PATTERN EXTRACTION SECTION
37
S1
D10, D13
AUTHENTICATION SECTION
38
ATCD
TERMINAL ANTENNA
23
TRANS-MISSION/ RECEPTION SECTION
D4, D6
D8
27
TERMINAL CPU
21
D13, D12
ROM
RAM
EEPROM
22
D3, D11
ENCRYPTION/ DECRYPTION SECTION
24
D2, D7
RANDOM NUMBER GENERATION SECTION
25

FIG. 5

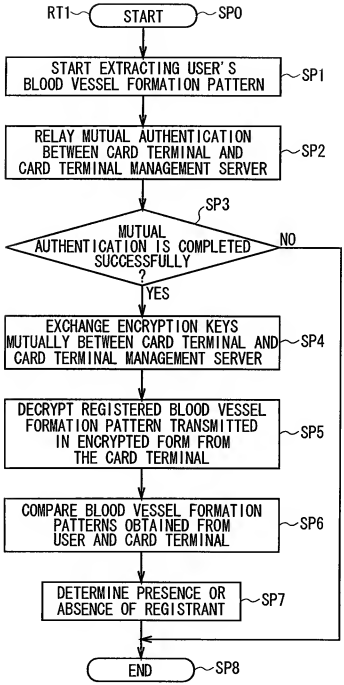

RT1
START
SP0
START EXTRACTING USER'S BLOOD VESSEL FORMATION PATTERN
SP1
RELAY MUTUAL AUTHENTICATION BETWEEN CARD TERMINAL AND CARD TERMINAL MANAGEMENT SERVER
SP2
SP3
MUTUAL AUTHENTICATION IS COMPLETED SUCCESSFULLY ?
NO
YES
EXCHANGE ENCRYPTION KEYS MUTUALLY BETWEEN CARD TERMINAL AND CARD TERMINAL MANAGEMENT SERVER
SP4
DECRYPT REGISTERED BLOOD VESSEL FORMATION PATTERN TRANSMITTED IN ENCRYPTED FORM FROM THE CARD TERMINAL
SP5
COMPARE BLOOD VESSEL FORMATION PATTERNS OBTAINED FROM USER AND CARD TERMINAL
SP6
DETERMINE PRESENCE OR ABSENCE OF REGISTRANT
SP7
END
SP8

FIG. 6

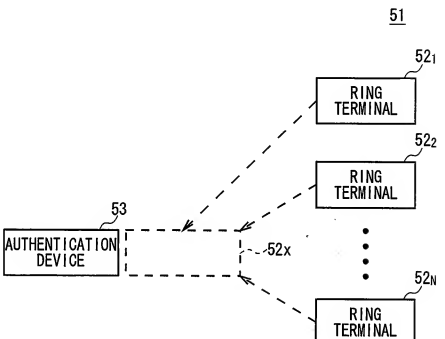

51
52₁
RING TERMINAL
52₂
RING TERMINAL
53
AUTHENTICATION DEVICE
52x
52N
RING TERMINAL

FIG. 7

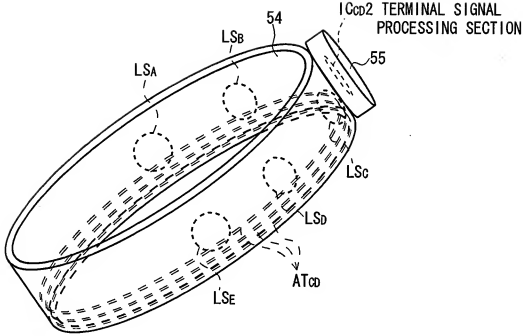

54
ICCD2 TERMINAL SIGNAL
PROCESSING SECTION
LSB
55
LSA
LSC
LSD
ATCD
LSE

FIG. 8

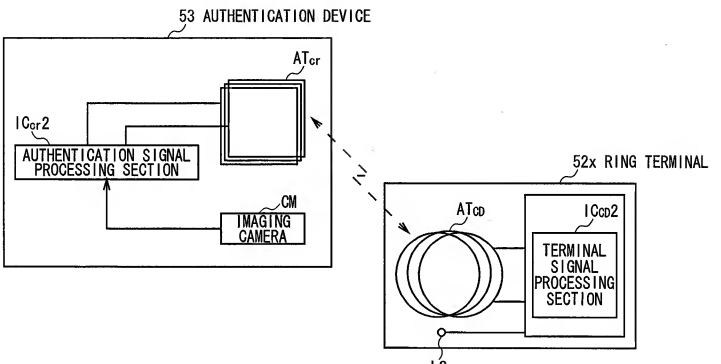

53 AUTHENTICATION DEVICE
ATcr
ICcr2
AUTHENTICATION SIGNAL PROCESSING SECTION
CM
IMAGING CAMERA
52x RING TERMINAL
ATcD
ICcD2
TERMINAL SIGNAL PROCESSING SECTION
LS

FIG. 9

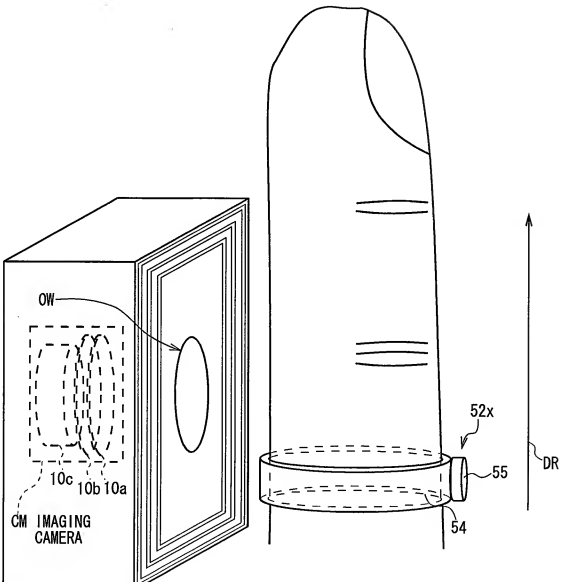


FIG. 10

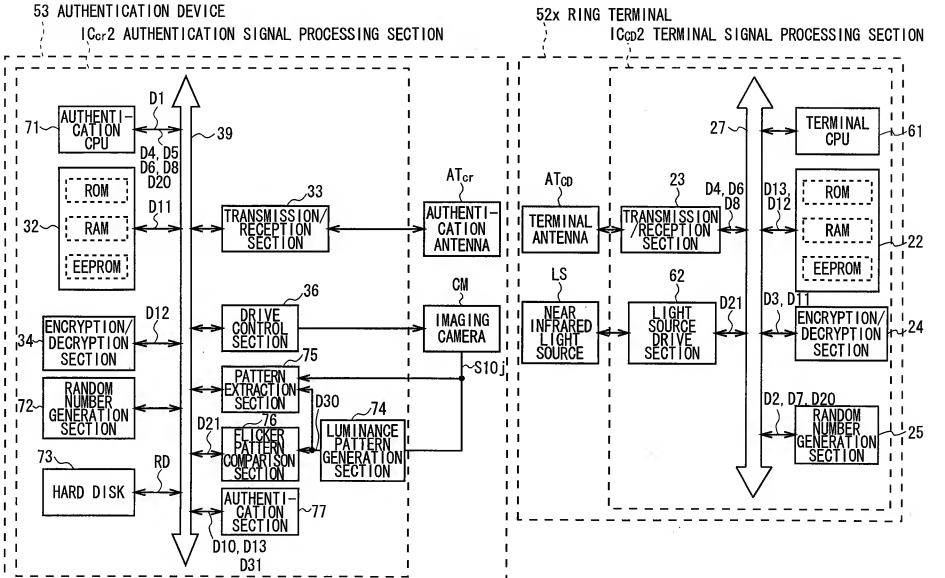

53 AUTHENTICATION DEVICE
ICcr2 AUTHENTICATION SIGNAL PROCESSING SECTION
52x RING TERMINAL
ICcd2 TERMINAL SIGNAL PROCESSING SECTION
AUTHENTI-CATION CPU
71
D1
D4, D5
D6, D8
D20
39
ROM
RAM
EEPROM
32
D11
TRANSMISSION/RECEPTION SECTION
33
ATcr
AUTHENTI-CATION ANTENNA
ATcd
TERMINAL ANTENNA
23
D4, D6
D8
TRANSMISSION/RECEPTION SECTION
27
TERMINAL CPU
61
D13, D12
ROM
RAM
EEPROM
22
ENCRYPTION/DECRYPTION SECTION
34
D12
DRIVE CONTROL SECTION
36
CM
IMAGING CAMERA
S10j
LS
NEAR INFRARED LIGHT SOURCE
62
LIGHT SOURCE DRIVE SECTION
D21
D3, D11
ENCRYPTION/DECRYPTION SECTION
24
RANDOM NUMBER GENERATION SECTION
72
PATTERN EXTRACTION SECTION
75
D30
74
LUMINANCE PATTERN GENERATION SECTION
D21
FLICKER PATTERN COMPARISON SECTION
76
D2, D7, D20
RANDOM NUMBER GENERATION SECTION
25
73
HARD DISK
RD
AUTHENTI-CATION SECTION
77
D10, D13
D31

FIG. 11

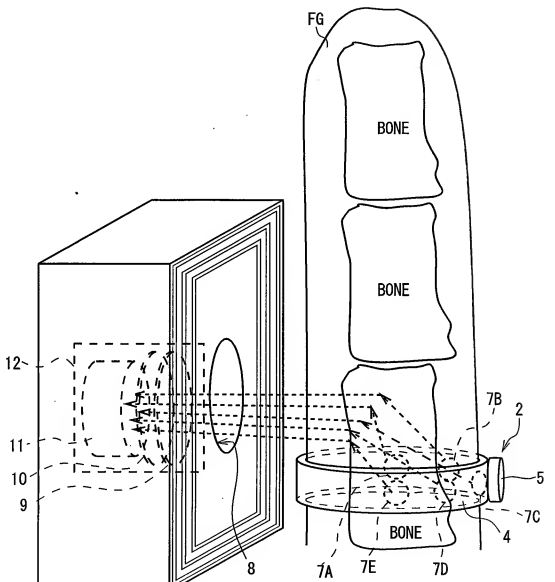


FIG. 12

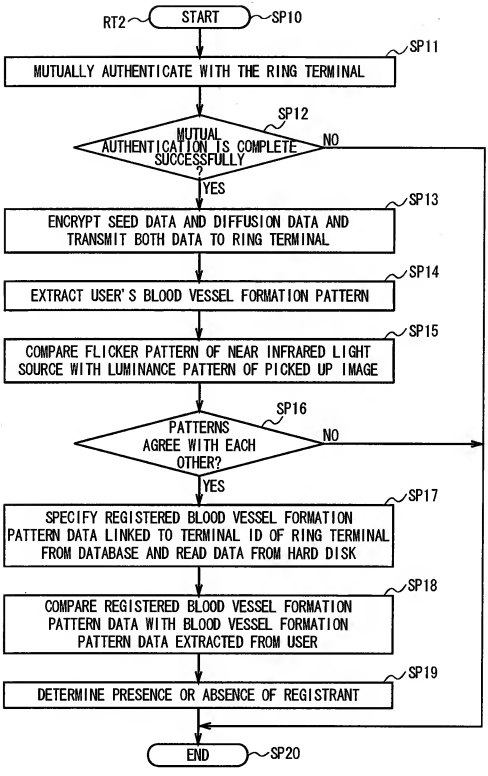

RT2
START
SP10
SP11
MUTUALLY AUTHENTICATE WITH THE RING TERMINAL
SP12
MUTUAL AUTHENTICATION IS COMPLETE SUCCESSFULLY?
NO
YES
SP13
ENCRYPT SEED DATA AND DIFFUSION DATA AND TRANSMIT BOTH DATA TO RING TERMINAL
SP14
EXTRACT USER'S BLOOD VESSEL FORMATION PATTERN
SP15
COMPARE FLICKER PATTERN OF NEAR INFRARED LIGHT SOURCE WITH LUMINANCE PATTERN OF PICKED UP IMAGE
SP16
PATTERNS AGREE WITH EACH OTHER?
NO
YES
SP17
SPECIFY REGISTERED BLOOD VESSEL FORMATION PATTERN DATA LINKED TO TERMINAL ID OF RING TERMINAL FROM DATABASE AND READ DATA FROM HARD DISK
SP18
COMPARE REGISTERED BLOOD VESSEL FORMATION PATTERN DATA WITH BLOOD VESSEL FORMATION PATTERN DATA EXTRACTED FROM USER
SP19
DETERMINE PRESENCE OR ABSENCE OF REGISTRANT
END
SP20

FIG. 13

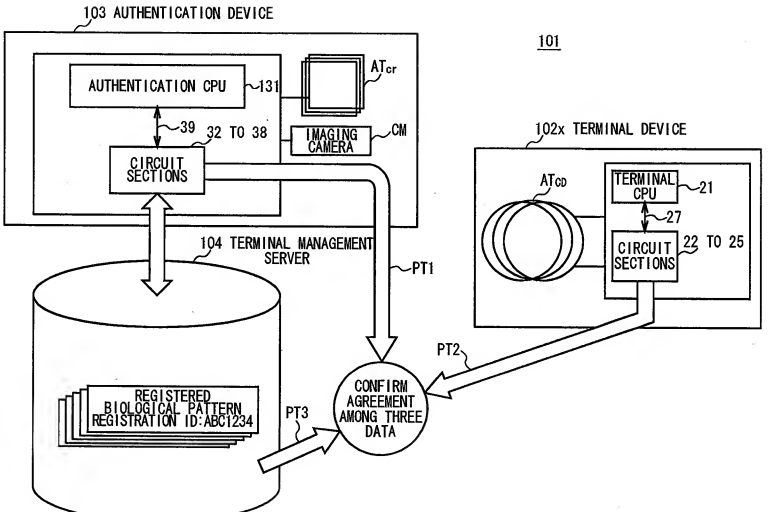

103 AUTHENTICATION DEVICE
101
AUTHENTICATION CPU
131
ATcr
39
32 TO 38
IMAGING CAMERA
CM
CIRCUIT SECTIONS
102x TERMINAL DEVICE
ATcp
TERMINAL CPU
21
27
CIRCUIT SECTIONS
22 TO 25
104 TERMINAL MANAGEMENT SERVER
PT1
PT2
REGISTERED BIOLOGICAL PATTERN REGISTRATION ID:ABC1234
PT3
CONFIRM AGREEMENT AMONG THREE DATA

FIG. 14

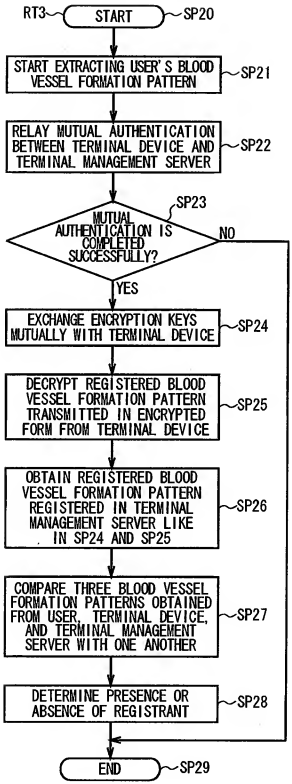

RT3
START
SP20
START EXTRACTING USER'S BLOOD VESSEL FORMATION PATTERN
SP21
RELAY MUTUAL AUTHENTICATION BETWEEN TERMINAL DEVICE AND TERMINAL MANAGEMENT SERVER
SP22
SP23
MUTUAL AUTHENTICATION IS COMPLETED SUCCESSFULLY?
NO
YES
EXCHANGE ENCRYPTION KEYS MUTUALLY WITH TERMINAL DEVICE
SP24
DECRYPT REGISTERED BLOOD VESSEL FORMATION PATTERN TRANSMITTED IN ENCRYPTED FORM FROM TERMINAL DEVICE
SP25
OBTAIN REGISTERED BLOOD VESSEL FORMATION PATTERN REGISTERED IN TERMINAL MANAGEMENT SERVER LIKE IN SP24 AND SP25
SP26
COMPARE THREE BLOOD VESSEL FORMATION PATTERNS OBTAINED FROM USER, TERMINAL DEVICE, AND TERMINAL MANAGEMENT SERVER WITH ONE ANOTHER
SP27
DETERMINE PRESENCE OR ABSENCE OF REGISTRANT
SP28
END
SP29

FIG. 15

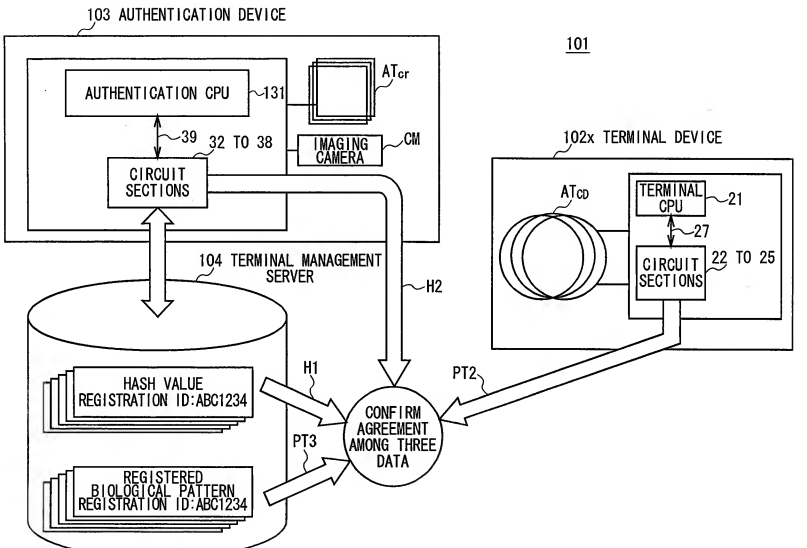

103 AUTHENTICATION DEVICE
101
AUTHENTICATION CPU
131
ATcr
39
32 TO 38
IMAGING CAMERA
CM
CIRCUIT SECTIONS
102x TERMINAL DEVICE
ATcd
TERMINAL CPU
21
27
CIRCUIT SECTIONS
22 TO 25
104 TERMINAL MANAGEMENT SERVER
H2
HASH VALUE REGISTRATION ID:ABC1234
H1
PT2
CONFIRM AGREEMENT AMONG THREE DATA
PT3
REGISTERED BIOLOGICAL PATTERN REGISTRATION ID:ABC1234

FIG. 16

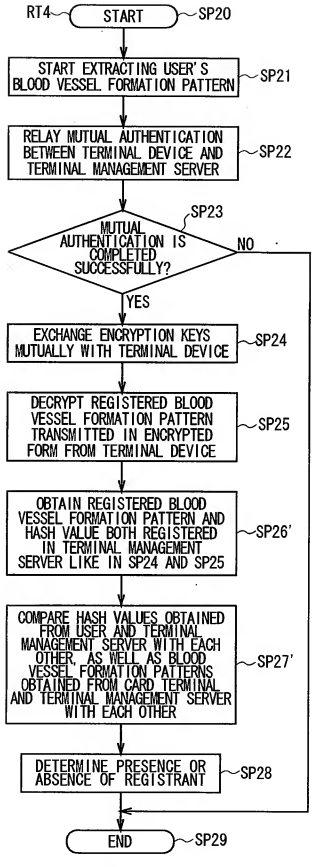

RT4
START
SP20
START EXTRACTING USER'S BLOOD VESSEL FORMATION PATTERN
SP21
RELAY MUTUAL AUTHENTICATION BETWEEN TERMINAL DEVICE AND TERMINAL MANAGEMENT SERVER
SP22
SP23
MUTUAL AUTHENTICATION IS COMPLETED SUCCESSFULLY?
NO
YES
EXCHANGE ENCRYPTION KEYS MUTUALLY WITH TERMINAL DEVICE
SP24
DECRYPT REGISTERED BLOOD VESSEL FORMATION PATTERN TRANSMITTED IN ENCRYPTED FORM FROM TERMINAL DEVICE
SP25
OBTAIN REGISTERED BLOOD VESSEL FORMATION PATTERN AND HASH VALUE BOTH REGISTERED IN TERMINAL MANAGEMENT SERVER LIKE IN SP24 AND SP25
SP26'
COMPARE HASH VALUES OBTAINED FROM USER AND TERMINAL MANAGEMENT SERVER WITH EACH OTHER, AS WELL AS BLOOD VESSEL FORMATION PATTERNS OBTAINED FROM CARD TERMINAL AND TERMINAL MANAGEMENT SERVER WITH EACH OTHER
SP27'
DETERMINE PRESENCE OR ABSENCE OF REGISTRANT
SP28
END
SP29

FIG. 17

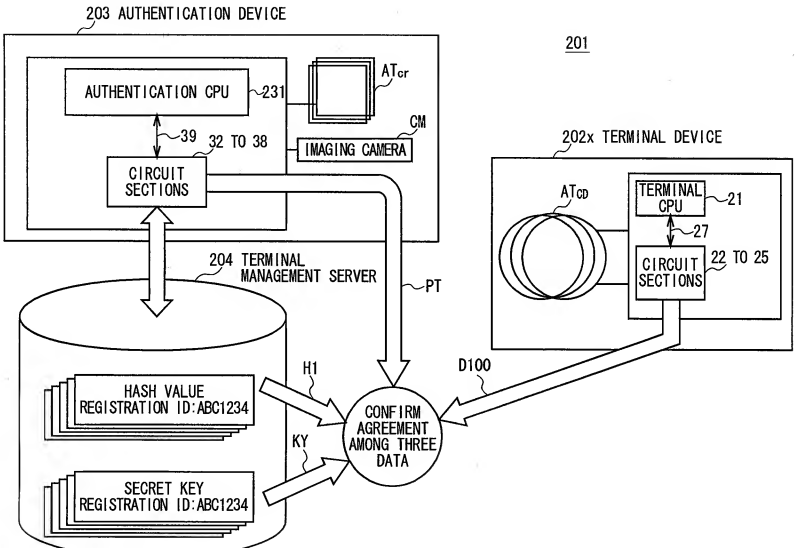

203 AUTHENTICATION DEVICE
201
AUTHENTICATION CPU
231
ATcr
39
32 TO 38
CM
IMAGING CAMERA
CIRCUIT SECTIONS
202x TERMINAL DEVICE
ATcp
TERMINAL CPU
21
27
CIRCUIT SECTIONS
22 TO 25
204 TERMINAL MANAGEMENT SERVER
PT
H1
D100
HASH VALUE REGISTRATION ID:ABC1234
CONFIRM AGREEMENT AMONG THREE DATA
KY
SECRET KEY REGISTRATION ID:ABC1234

FIG. 18

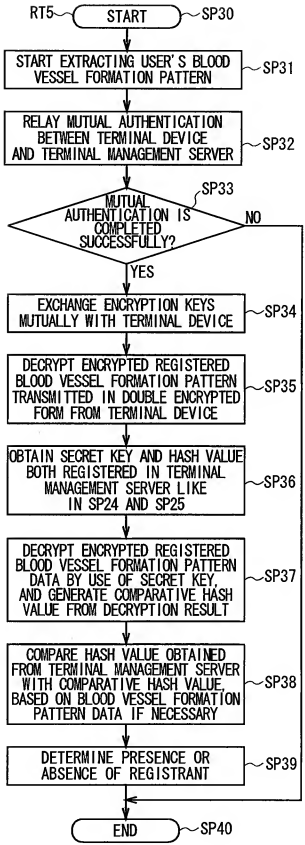
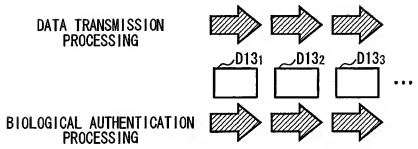

RT5
START
SP30
START EXTRACTING USER'S BLOOD VESSEL FORMATION PATTERN
SP31
RELAY MUTUAL AUTHENTICATION BETWEEN TERMINAL DEVICE AND TERMINAL MANAGEMENT SERVER
SP32
SP33
MUTUAL AUTHENTICATION IS COMPLETED SUCCESSFULLY?
NO
YES
EXCHANGE ENCRYPTION KEYS MUTUALLY WITH TERMINAL DEVICE
SP34
DECRYPT ENCRYPTED REGISTERED BLOOD VESSEL FORMATION PATTERN TRANSMITTED IN DOUBLE ENCRYPTED FORM FROM TERMINAL DEVICE
SP35
OBTAIN SECRET KEY AND HASH VALUE BOTH REGISTERED IN TERMINAL MANAGEMENT SERVER LIKE IN SP24 AND SP25
SP36
DECRYPT ENCRYPTED REGISTERED BLOOD VESSEL FORMATION PATTERN DATA BY USE OF SECRET KEY, AND GENERATE COMPARATIVE HASH VALUE FROM DECRYPTION RESULT
SP37
COMPARE HASH VALUE OBTAINED FROM TERMINAL MANAGEMENT SERVER WITH COMPARATIVE HASH VALUE BASED ON BLOOD VESSEL FORMATION PATTERN DATA IF NECESSARY
SP38
DETERMINE PRESENCE OR ABSENCE OF REGISTRANT
SP39
END
SP40

FIG. 19

(A) NO COMMUNICATION ERRORS



(B) COMMUNICATION ERROR D13₂

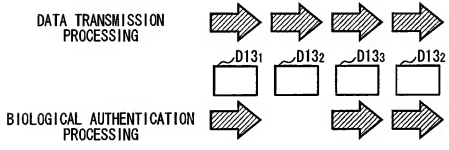


FIG. 20

EXPLANATION OF REFERENCED NUMERALS

1, 51, 101, 201……INFORMATION PROCESSING SYSTEM, 2i (i=1, 2, ……, N), 2x……CARD TERMINAL, 52i (i=1, 2, ……, N), 52x……RING TERMINAL, 102x, 202x……TERMINAL DEVICE, 3, 53, 103, 203……AUTHENTICATION DEVICE, 4……CARD TERMINAL MANAGEMENT SERVER, 104, 204……TERMINAL MANAGEMENT SERVER, 21, 61……TERMINAL CPU, 31, 71, 131, 231……AUTHENTICATION CPU, 22, 32……INTERNAL MEMORY, 23, 33……TRANSMISSION/RECEPTION SECTION, 24, 34……ENCRYPTION/DECRYPTION SECTION, 25……RANDOM NUMBER GENERATION SECTION, 35……NETWORK INTERFACE, 36……DRIVE CONTROL SECTION, 37, 75……PATTERN EXTRACTION SECTION, 38, 77……AUTHENTICATION SECTION, 73……HARD DISK, 74……LUMINANCE PATTERN GENERATION SECTION, 76……FLICKER PATTERN COMPARISON SECTION, CM……IMAGING CAMERA, LS……NEAR INFRARED LIGHT SOURCE, ATCD……TERMINAL ANTENNA, ATcr……AUTHENTICATION ANTENNA, ICCD1, ICCD2……TERMINAL SIGNAL PROCESSING SECTION, ICcr1, ICcr2……AUTHENTICATION SIGNAL PROCESSING SECTION, RT1……FIRST AUTHENTICATION PROCESSING PROCEDURE, RT2……SECOND AUTHENTICATION PROCESSING PROCEDURE, RT3……THIRD AUTHENTICATION PROCESSING PROCEDURE, RT4……FOURTH AUTHENTICATION PROCESSING PROCEDURE, RT5……FIFTH AUTHENTICATION PROCESSING PROCEDURE